UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/442,727	11/18/1999	SADAHARU SATO	450100-02171	6321

20999 7590 03/08/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/442,727	SATO, SADAHARU	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-8 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-8 are rejected under 35 U.S.C. 102(e) as being anticipated by Iitsuka et al, U.S. Patent 6,463,151.

As per claim 1, it is disclosed by Iitsuka et al of a signal processing circuit for transmitting data as packet data to a serial interface bus in a predetermined time cycle (col. 8, lines 20-25; col. 9, lines 49-56; and col. 11, lines 12-16). A cipher circuit for enciphering the data to be transmitted by a predetermined cipher mode (col. 8, lines 38-58). One of the cipher modes includes a copy once prohibition mode wherein data cannot be reproduced more than once (col. 9, lines 33-48). A transmission circuit adds enciphering information representative of the cipher mode to the data enciphered in the

cipher processing circuit and transmits the enciphering data and the enciphering information to the serial interface bus (col. 8, lines 38-58). It is determined whether the cipher mode and the enciphering information correspond and when the cipher mode and enciphering information are determined not to correspond, transmitting the data enciphered by a different cipher mode to the serial interface bus as packet data in another cycle (col. 8, lines 58-62; col. 10, lines 55-58; col. 11, lines 12-16; and col. 15, lines 22-56).

As per claim 2, Iitsuka et al teaches that the transmission circuit sets the enciphering information in a predetermined region of a header of the packet (col. 9, lines 36-41 and as shown in Figure 6 denoted as "Sy").

As per claim 3, the teachings of Iitsuka et al disclose of a signal processing circuit for transmitting data as packet data to a serial interface bus in a predetermined time cycle (col. 8, lines 20-25; col. 9, lines 49-56; and col. 11, lines 12-16). A holding means in which information of atleast one of a number of cipher modes is set (col. 8, lines 38-58). One of the cipher modes is a copy once prohibition mode wherein data can not be reproduced more than once (col. 9, lines 33-48). A control means specifies a cipher mode for enciphering the data for transmission (col. 8, lines 38-58). A cipher processing circuit including cipher mode selection circuit for accessing the cipher mode information specified by the control means from the holding means (col. 8, lines 38-58). A cipher engine circuit for enciphering the data to be transmitted in the cipher mode selected in the cipher mode selection circuit and outputting enciphered data (col. 8, lines 38-58). A transmission circuit adds enciphering information representative of the

cipher mode to the data enciphered in the cipher processing circuit and transmits the enciphering data and the enciphering information to the serial interface bus (col. 8, lines 38-58). It is determined whether the cipher mode and the enciphering information correspond and when the cipher mode and enciphering information are determined not to correspond, transmitting the data enciphered by a different cipher mode to the serial interface bus as packet data in another cycle (col. 8, lines 58-62; col. 10, lines 55-58; col. 11, lines 12-16; and col. 15, lines 22-56).

As per claim 4, Iitsuka et al teaches that the transmission circuit sets the enciphering information in a predetermined region of a header of the packet (col. 9, lines 36-41 and as shown in Figure 6 denoted as "Sy").

As per claim 5, it is disclosed by Iitsuka et al of a signal processing circuit for transmitting data as packet data to a serial interface bus in a predetermined time cycle (col. 8, lines 20-25; col. 9, lines 49-56; and col. 11, lines 12-16). It is disclosed of a storage means and holding means in which information of atleast one of a number of cipher modes is set (col. 8, lines 38-58). One of the cipher modes is a copy once prohibition mode wherein data can not be reproduced more than once (col. 9, lines 33-48). A control means specifies a cipher mode for enciphering the data for transmission (col. 8, lines 38-58). A cipher processing circuit including cipher mode selection circuit for accessing the cipher mode information specified by the control means from the holding means (col. 8, lines 38-58). A cipher engine circuit for enciphering the data to be transmitted in the cipher mode selected in the cipher mode selection circuit and outputting enciphered data (col. 8, lines 38-58). A first transmission circuit for

generating time information, adding to the time information the enciphering information, and storing the result in the storing means along with the enciphered data (col. 8, lines 38-62). A second transmission circuit for reading enciphered data to which has been added time information and enciphering information stored in the storing means (col. 8, lines 38-62). Generating packet data in a predetermined format, setting the enciphering information in the packet header, and transmitting the result to the serial interface bus (col. 9, lines 36-41,49-56 and as shown in Figure 6 denoted as "Sy"). When transmitting a plurality of packets, confirming continuity of the cipher mode from the enciphering information. Stopping the transmission when the cipher mode and the enciphering information are determined not to correspond even if there is room in a band enabling transmission in the predetermined time cycle and transmitting the data enciphered by a different cipher mode to the serial interface bus a packet data in a next cycle (col. 8, lines 58-62; col. 10, lines 55-58; col. 11, lines 12-16; and col. 15, lines 22-56).

As per claim 6, the teachings of Iitsuka et al disclose of a signal processing circuit for transmitting and receiving data as enciphered packet data to and from a serial interface bus in a predetermined time cycle (col. 8, lines 20-25; col. 9, lines 49-56; and col. 11, lines 12-16). A cipher circuit for enciphering the data to be transmitted by a predetermined cipher mode at the time of transmission (col. 8, lines 38-58). One of the cipher modes includes a copy once prohibition mode wherein data cannot be reproduced more than once (col. 9, lines 33-48). The received enciphered data is deciphered based on the enciphering information included in the packet at the time of

reception (col. 5, lines 20-48). A transmission circuit adds enciphering information representative of the cipher mode to the data enciphered in the cipher processing circuit and transmits the enciphering data and the enciphering information to the serial interface bus (col. 8, lines 38-58). Confirming the continuity of the cipher mode by the enciphering information when transmitting a plurality of packets and transmitting the data enciphered by a different cipher mode to the serial interface bus as packet data in another cycle when the cipher mode and the enciphering information are determined not to correspond (col. 8, lines 58-62; col. 10, lines 55-58; col. 11, lines 12-16; and col. 15, lines 22-56).

As per claim 7, Iitsuka et al teaches that the transmission circuit sets the enciphering information in a predetermined region of a header of the packet (col. 9, lines 36-41 and as shown in Figure 6 denoted as "Sy").

As per claim 8, Iitsuka et al discloses of a signal processing circuit for transmitting an receiving data as enciphered packet data to and from a serial interface bus in a predetermined time cycle (col. 8, lines 20-25; col. 9, lines 49-56; and col. 11, lines 12-16). It is taught of (first and second) storing means and holding means in which information of atleast one of a number of cipher modes is set (col. 8, lines 38-58). One of the cipher modes is a copy once prohibition mode wherein data can not be reproduced more than once (col. 9, lines 33-48). A control means for specifying a cipher mode for enciphering transmission data (col. 8, lines 38-58). A first reception circuit for storing time information, enciphering data, and the enciphering information of received packet data in the (first) storage means (col. 8, lines 38-62 and col. 13, lines

12-38). A second reception circuit for outputting the enciphering information and the enciphered data stored in the first storing means and indicating a time for outputting the received data based on the time information (col. 8, lines 38-58). A cipher processing circuit including a cipher mode detection circuit for detecting a cipher mode used for enciphering data by the enciphering information from the second reception circuit (col. 8, lines 38-58). A cipher mode selection circuit for accessing cipher mode information specified by the control means at the time of transmission and selecting the cipher mode information detected by the cipher mode detection circuit from the information set in the holding means at the time of reception (col. 8, lines 38-58). A cipher engine circuit for enciphering the data to be transmitted in the cipher mode accessed in the cipher selection circuit, outputting the enciphered data at the time of transmission, and deciphering the received data in the cipher mode accessed in the cipher mode selection circuit at the time of reception (col. 8, lines 38-58). A first transmission circuit for generating time information, adding to the time information the enciphering information, and storing the result in the storing means along with the enciphered data (col. 8, lines 38-58 and col. 13, lines 12-38). A second transmission circuit for reading enciphered data to which has been added time information and enciphering information stored in the storing means (col. 8, lines 38-62 and col. 13, lines 12-38). Generating packet data in a predetermined format, setting the enciphering information in the packet header, and transmitting the result to the serial interface bus (col. 9, lines 36-41,49-56 and as shown in Figure 6 denoted as "Sy"). When transmitting a plurality of packets, confirming continuity of the cipher mode from the enciphering information. Stopping the

transmission when the cipher mode and the enciphering information are determined not to correspond even if there is room in a band enabling transmission in the predetermined time cycle and transmitting the data enciphered by a different cipher mode to the serial interface bus a packet data in a next cycle (col. 8, lines 58-62; col. 10, lines 55-58; col. 11, lines 12-16; and col. 15, lines 22-56).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Inoue et al, U.S. Patent 6,467,093 is a related teaching by the applicant.

Sato et al, U.S. Patent 6,463,060 is a related teaching by the applicant.

Sato, U.S. Patent 6,408,012 is a related teaching by the applicant.

Sato et al, U.S. Patent 6,259,694 is a related teaching by the applicant.

Iitsuka et al, EP 0913975 discloses of cipher modes for encrypting data.

"IEEE Standard for High Performance Serial Bus" discloses of the standard for IEEE 1394 serial buses.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

3/5/05

CR
March 5, 2005